Title: Security containers and access rights in HelenOS
Author: Štěpán Henek
Department: Department of Software Engineering
Supervisor: Mgr. Martin Děcký
Supervisor's e-mail address: decky@ksi.mff.cuni.cz

Abstract: The goal of this thesis is to design and implement security containers (contexts) for tasks and access rights mechanisms for microkernel operating systems.
The access rights mechanisms implement common paradigms such as user identification, groups of users, system entities (tasks, files) ownership, user capabilities and access control lists.
Moreover, the design allows to implement hierarchical security domains, where each domain is able to delegate a subset of its permissions to its subdomains. The design also enables the implementation of containers, which mutually isolate those tasks, which are situated in security domains with an empty intersection.
The thesis comprises of an analysis and evaluation of possible approaches, a prototype implementation in HelenOS with respect to its specific properties (emphasis on a small context switch overhead, delegation of security mechanisms to privileged user space tasks, etc.) and also comparison with implementations of security containers and access rights mechanisms in generally available operating systems.

Keywords: security contexts, access rights, microkernel, HelenOS